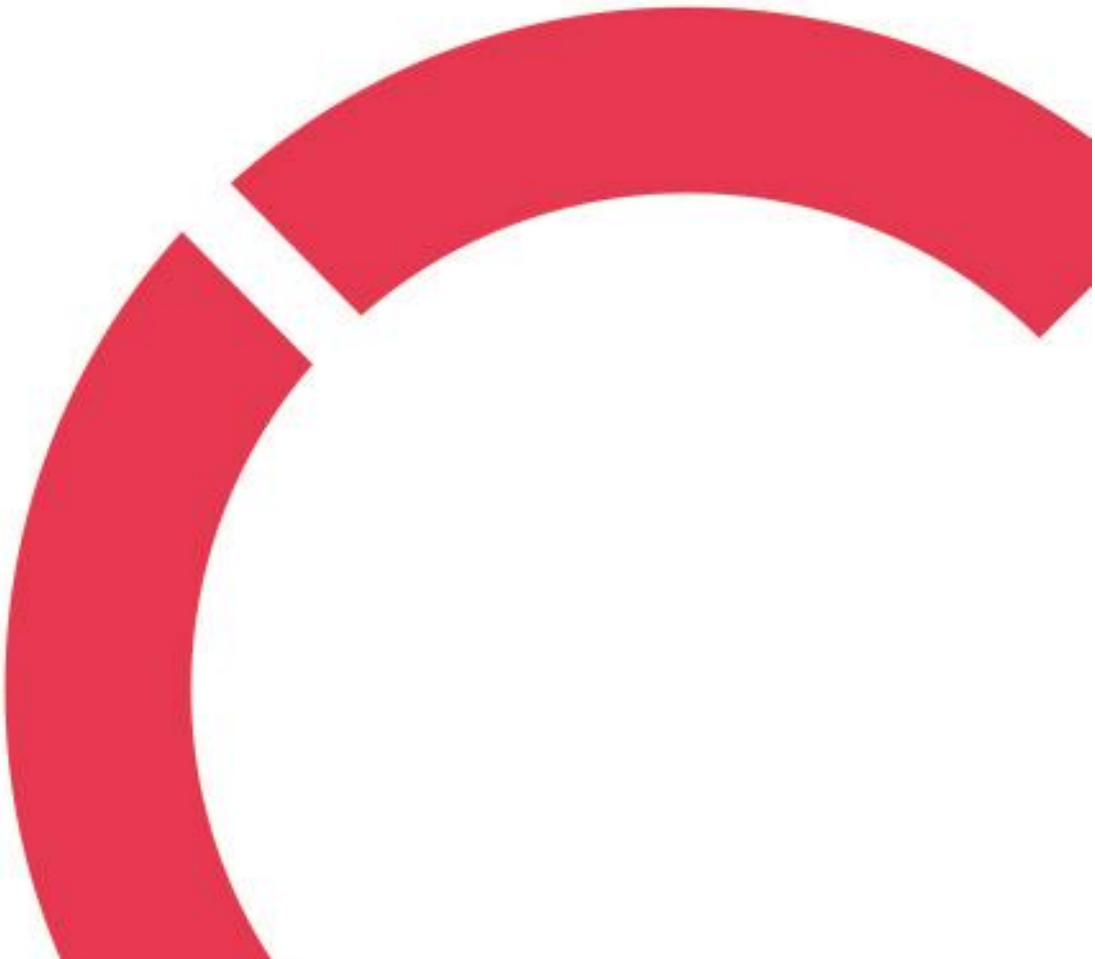
Susanna Rinne

KYBERHYÖKKÄYSTEN TUNNISTAMINEN JA TORJUMINEN VERKOSSA

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Toukokuu 2023



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Toukokuu 2023	**Tekijä/tekijät** Susanna Rinne
Koulutus Tieto- ja viestintätekniikan koulutus		☒ AMK ☐ YAMK
Työn nimi KYBERHYÖKKÄYSTEN TUNNISTAMINEN JA TORJUMINEN VERKOSSA.		
Työn ohjaaja Jari Isohanni		**Sivumäärä** 27
Työelämäohjaaja -		

Tässä opinnäytetyössä tutustuttiin verkossa tapahtuviin kyberhyökkäyksiin ja niiden tunnistukseen ja torjuntaan. Tämän opinnäytetyön pääasiallisena tavoitteena oli lisätä tietämystä erilaisista kyberhyökkäyksistä. Opinnäytetyöllä haluttiin luoda selkeä kokonaisuus, jossa esitellään kyberhyökkäystyyppejä ja niiden torjuntaa helposti ymmärrettävällä tavalla samalla avaten aiheeseen liittyviä termejä. Opinnäytetyössä kyberhyökkäysten tutkintaan sovellettiin erilaisia kirjoja ja verkkomateriaaleja, jotka käsittelivät aiheita liittyen kyberhyökkäyksiin ja kyberturvallisuuteen. Opinnäytetyössä aihetta tutkittiin täysin teoriaan pohjautuen.

Opinnäytetyön alussa tutkittiin yleistasolla kyberhyökkääjiä ja erilaisia kyberhyökkäysten tyyppejä. Työssä perehdyttiin tarkemmin kyberhyökkäysten toimintaperiaatteisiin, leviämistapoihin ja vaikutuksiin, joiden pohjalta kyberhyökkäyksiä pystytään tunnistamaan verkossa. Opinnäytetyössä pyrittiin käsittelemään mahdollisimman kattava osa yleisimmistä kyberhyökkäyksistä. Opinnäytetyön lopussa tutkittiin vielä yleisiä keinoja kyberhyökkäysten torjuntaan. Tässä osiossa perehdyttiin erilaisiin kyberturvallisuutta vahvistaviin verkon käyttäjän toimintatapoihin ja suojaukseen suunniteltuihin verkkotyökaluihin. Opinnäytetyössä torjuntakeinoja käsiteltiin tarkemmin käymällä läpi teoriaa niiden toimintaperiaatteista ja vaikutuksista.

Yleisesti tämän opinnäytetyön kautta saatiin lisää tietoa kyberhyökkäyksien ominaisuuksista ja pystyttiin tuomaan esiin paremmin hyökkäysten vaikutusten laajuutta ja merkitystä verkon käyttäjille. Opinnäytetyön lopputuloksena saatiin informatiivinen kokonaisuus, jossa kerrotaan tiivistetysti tärkeimpiä pääpiirteitä erilaisista kyberhyökkäyksistä.

Asiasanat
haittaohjelmat, kyberhyökkäykset, kyberhyökkääjät, palvelunestohyökkäykset

ABSTRACT

Centria University of Applied Sciences	Date May 2023	Author Susanna Rinne
Degree programme Information and communication technology		
Name of thesis IDENTIFYING AND PREVENTING CYBERATTACKS ONLINE.		
Centria supervisor Jari Isohanni		**Pages** 27
Instructor representing commissioning institution or company -		

This thesis studied cyber attacks and their identification and prevention online. The main goal of this thesis was to increase knowledge about cyber attacks of a different kind. Also, the aim of this thesis was to create a clear study that presents different types of cyber attacks and their prevention methods in an easy-to-understand way, while opening the terms related to the topic. In the thesis, various books and online materials related to cyber attacks and cyber security were applied to the research. In the thesis, the subject was studied completely based on theory.

The beginning part of the thesis examined cyber attackers and different types of cyber attacks on a general level. The thesis studied in more detail the operating principles of cyber attacks, spreading techniques and influence that can be used to identify the cyber attacks online. Thesis attempt to cover as comprehensively as possible a part of the most common cyber attacks. The end part of the thesis studied the general ways to prevent cyber attacks. In this section, the thesis examined various network user action that strength cyber security and network tools that are designed to secure network. The thesis studied in more detail the different ways to prevent cyber attacks by going through theory about the operating principles of prevention and their influence.

In general, this thesis provides more information about the characteristics of cyber attacks and highlights better the extent of the influence of cyber attacks and their meaning to web users. The result of the thesis was an informative study that summarizes the main features of cyber attacks of a different kind.

Key words
cyber attackers, cyber attacks, denial of service, malware

KÄSITTEIDEN MÄÄRITTELY

BROADCAST-OSOITE

Verkko-osoite, joka on tarkoitettu yleislähetykseen. Tätä verkko-osoitetta käytetään silloin, kun lähetyksen kohteena halutaan käyttää kaikkia laitteita tietyssä verkossa.

DOM (Document Object Model)

Verkkodokumenttien ohjelmointirajapinta, jonka avulla esitetään HTML- ja XML-dokumenttien rakennetta puukaaviona. DOM:n kautta dokumenttien rakennetta voidaan tutkia ja muuttaa.

ECHO REQUEST

ICMP:n ping-komennolla toteutettava pyyntö, jonka avulla selvitetään toiseen laitteen saavutettavuus verkossa. Vastaanottava laite vastaa echo request -pyyntöön echo reply -viestillä.

ICMP (Internet Control Message Protocol)

Protokolla, jolla verkon laiteet voivat välittää toisilleen informaatiota ja virheilmoituksia verkon tilasta.

IP-OSOITE

Verkkoon liitettyjen laitteiden yksilöllinen osoite, jonka avulla laite tunnistetaan verkossa. Osoite perustuu Internet Protocol -reititysprotokollaan.

HTTP (Hypertext Transfer Protocol)

Protokolla, joka vastaa tiedonsiirrosta verkon selaimien ja www-palvelimen välillä.

HYÖKKÄYSPINTA-ALA

Kokonaisuus, joka kattaa kaikki hyökkäykselle haavoittuvaiset kohteet verkon laitteissa, järjestelmissä ja itse verkossa.

KAISTANLEVEYS

Verkon kapasiteetti datan kantamiselle. Kertoo datan määrän, joka pystytään siirtämään verkossa pakasta toiseen tietyssä ajassa.

KEYLOGGER

Ohjelma, joka seuraa ja tallentaa laitteelle annettuja näppäinsyötteitä.

KONFIGUROINTI

Toimenpiteet, joilla verkon laitteiden ja ohjelmistojen asetukset määritetään, säädetään ja otetaan käyttöön.

KRYPTAUS

Datan salaamista erilaisten salaustekniikoiden avulla.

KYBERTURVALLISUUS

Turvallisuuden osa-alue, jolla tarkoitetaan kaikkia teknisen turvallisuuden toimia verkkojen, laitteiden ja digitaalisen datan suojaamisessa.

LDAP (Lightweight Directory Access Protocol)

Protokolla, jota käytetään hakemistopalvelussa, kuten käyttäjähakemistoissa, joilla voidaan toteuttaa käyttäjien tunnistusta.

OGNL (Object-Graph Navigation Language)

Ilmaisukieli, jota käytetään hakemaan ja asettamaan ominaisuuksia Java-ohjelmointikielellä luoduissa objekteissa.

ORM (Object Relational Mapping)

Tekniikka, joka mahdollistaa tietokantojen datan käsittelyn objekteja hyödyntävillä ohjelmointikielillä ilman SQL-kyselyjä.

PING-KOMENTO

ICMP:n komento, jolla verkon laite voi tarkistaa toiseen laitteen saavutettavuuden verkossa.

PALVELIN

Palvelinohjelmistoja sisältävä tietokone, jonka tehtävänä on tarjota informaatiota ja erilaisia palveluja verkon muille laitteille.

PROTOKOLLA

Määrittää tietyt säännökset ja toimintatavat tietojen siirtämiselle Internetissä eri verkkojen, järjestelmien ja verkkokomponenttien välillä.

SPÄMMI

Ei toivottua viestintä sisältöä kuten roskapostia, mainoksia tai muita turhia viestejä.

SQL (Structured Query Language)

Tietokantojen hallintaan ja käsittelyyn suunniteltu kyselykieli.

SYN (Synchronize)

Paketti, jota käytetään osana TCP-yhteyden luomista käyttäjän ja palvelimen välillä.

TCP (Transmission Control Protocol)

Yhteydellinen kuljetusprotokolla, joka määrittää toimintatavat datan siirrolle verkossa samalla varmistaen siirretyn datan eheyden ja luotettavuuden.

UDP (User Datagram Protocol)

Yhteydetön kuljetusprotokolla, joka määrittää toimintatavat datan siirrolle verkossa mutta ei varmista siirretyn datan eheyttä ja luotettavuutta.

URL (Uniform Resource Location)

Verkko-osoite, joka kertoo tietyn sivuston tai tiedoston sijainnin verkossa.

VERKKOKERROS

Verkon rakennetta kuvaava osa-alue, jossa tapahtuu tietyt verkon toimenpiteet. Verkkokerroksia on OSI-mallin mukaan seitsemän, jotka ovat fyysinen, siirtoyhteys-, verkko-, kuljetus-, istunto-, esitystapa- ja sovelluskerros. Verkon tietoliikenteen käsittely ja liikkuminen tapahtuvat eri verkkokerrosten välillä.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVAT

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tutustua verkossa vaikuttaviin kyberhyökkäyksiin ja niiden tunnistukseen ja torjumiseen. Kyberhyökkäykset ovat nykypäivänä yleisiä ja melkein kaikki verkon käyttäjät joutuvat tekemisiin niiden kanssa tavalla tai toisella. Tämän takia kattava perustason tietämys erilaisista kyberhyökkäyksistä on oleellista, jotta verkon käyttämisestä voidaan tehdä mahdollisimman turvallista kaikille. Tämän oppinäytetyön ajatuksena on tutkia tarkemmin sitä, millaisia kyberhyökkäyksiä verkossa esiintyy ja millaisia variaatioita niistä löytyy.

Erilaisten kyberhyökkäystyyppien tutkinnan ohella opinnäytetyössä halutaan ottaa lyhyt katsaus siihen, millaisia tekijöitä ja tavoitteita hyökkäysten taustalla toimii. Lisäksi opinnäytetyössä käydään läpi, miten verkossa esiintyvät kyberhyökkäykset käytännössä toimivat ja millaiset vaikutukset niillä on verkkoon ja sen laitteiden toimintaan. Opinnäytetyön tavoitteena on selvittää, miten verkon käyttäjä voi tunnistaa erilaiset hyökkäykset ja välttää niiden kohteeksi joutumisen. Lopuksi opinnäytetyössä tutkitaan, millaisia vaihtoehtoja kyberhyökkäysten torjuntaan on saatavilla.

Tämän opinnäytetyön tutkimus pohjautuu täysin kyberturvallisuutta ja kyberhyökkäyksiä käsitteleviin kirjallisiin aineistoihin ja verkkomateriaaleihin. Opinnäytetyön keskeisinä käsitteinä ovat kyberhyökkäyksen mallit, toiminta ja hyökkäyksiltä suojautuminen. Opinnäytetyön päätavoitteena on tutkia erilaisia kyberhyökkäyksiä ja niiden toiminnan tunnistamista ja torjumista. Opinnäytetyön tarkoituksena on avata kyberhyökkäyksiin liittyviä käsitteitä ja antaa kattava kuva yleisimmistä kyberhyökkäyksistä, joita nykypäivänä tapahtuu verkossa.

2 YLEISESTI KYBERHYÖKKÄYKSISTÄ

Kyberhyökkäys on termi, jolla tarkoitetaan verkossa tai verkon välityksellä tapahtuvaa hyökkäystä. Hyökkäyksen tavoitteena on aiheuttaa vahinkoa verkossa järjestelmille ja käyttäjille. Kyberhyökkäyksen aiheuttama vahinko voi olla mitä vaan verkon häirinnästä ja lamauttamisesta aina arvokkaan datan varastamiseen tai tuhoamiseen. Yleisesti kyberhyökkäysten tarkoituksena on hyödyntää verkon haavoittuvuuksia ja päästä käsiksi erilaiseen dataan verkossa. Kyberhyökkäyksen toiminta ja tavoitteet vaihtelevat hyökkääjän mielenkiinnon kohteiden ja käytetyn hyökkäyksen mukaan.

Kyberhyökkäykset ovat jatkuvassa kehityksessä ja niiden määrä kasvaa nopeasti verkon ja sen palveluiden laajentumisen mukana. Nykypäivänä verkosta on tullut tärkeä osa monia elämän osa-alueita, kun yhä useammat perinteisistä palveluista ovat siirtyneet verkkoon. Verkon käyttöä on lisännyt myös se, että siitä on kehittynyt erittäin nopea ja tehokas tapa viestiä ja jakaa monipuolista dataa. (Bijalwan 2022, 3-4.) Uusia laitteita ja käyttäjiä liittyy verkkoon ripeällä tahdilla, minkä seurauksena myös kyberhyökkäyksiä mahdollistava hyökkäyspinta-ala laajentuu voimakkaasti (Singh 2020, 3). Laaja hyökkäyspinta-ala luo kyberhyökkääjille aina vain monipuolisemman ympäristön hyökkäysten tehtailuun samalla kun verkon tarjoamat innovaatiot ja globaalit yhteyden helpottavat kyberhyökkäysten toteuttamista (Singh 2020, 5-6).

Kyberhyökkäyksistä on muodostunut yleinen ongelma ja niiden vaikutukset näkyvät kaikille verkon käyttäjille. Hyökkäyksen kohteeksi voivat joutua niin yksityiset verkonkäyttäjä kuin yritykset. Perustason ymmärrys kyberhyökkäyksistä tulee siis tarpeelliseksi taidoksi jokaiselle verkon käyttäjälle. Tietoisuutta kyberhyökkäysten tuottamista uhista tarvitaan, jotta verkon käyttäjä voi arvioida hyökkäysten todennäköisyyttä ja tehdä tarvittavia toimia niiden välttämiseksi. Kyberhyökkäyksistä ajan tasalla pysyminen on kuitenkin haastava tehtävä päivittäin muuttuvassa verkkoympäristössä. (Waschke 2017, 2.) Kyberhyökkäysten tunnistamista hankaloittaa myös se, että hyökkäykset pystyvät hyödyntämään monipuolisesti eri alustoja toimintansa toteuttamiseen. Hyökkäys voi tapahtua verkkosivujen, sovellusten, sähköpostin ja monien muiden alustojen kautta. Lisäksi kyberhyökkäykset ovat erittäin monimuotoisia ja niitä voidaan käyttää ennennäkemättömillä tavoilla haavoittuvuuksiin verkossa. Nykyisessä kyberturvallisuustilanteessa kyberhyökkääjillä on käytössään valtava määrä erilaisia kyberuhkia, työkaluja ja metodeja hyökkäysten toteuttamiseen (Singh 2020, 13).

3 KYBERHYÖKKÄÄJÄT

Kyberhyökkääjä on tekijä, joka vastaa kyberhyökkäyksen toteuttamisesta. Kyberhyökkääjä tutkii haavoittuvuuksia, suunnittelee hyökkäystä ja valitsee tarvittavat työkalut ja metodit hyökkäyksen suorittamiseen. Kyberhyökkääjinä voivat toimia niin yksittäiset henkilöt kuin pienet ryhmät. Hyökkääjä voi toimia myös osana suurempaa organisaatiota tai työskennellä valtiollisen tahon alaisuudessa. Kyberhyökkäyksen kohde ja käytetty hyökkäyksen muoto riippuvat hyökkääjän motiiveista ja tavoitteista. Kyberhyökkääjä voi toimia sotilaallisen, taloudellisen, markkinallisen tai terroristisen tavoitteen motivoiman. Kyberhyökkäyksen syy voi pohjautua myös huomion hakemiseen verkossa, vakoiluun tai tietojen varastamiseen. (Bijalwan 2022, 33-35.) Motiivit kyberhyökkäyksille ovat yhtä vaihtelevia kuin niiden takana toimivat kyberhyökkääjät ja heidän profiilinsa (Waschke 2017, 5).

Kyberhyökkääjille on olemassa omia luokituksia, jotka perustuvat hyökkääjän toimitaan ja suorittamiin hyökkäyksiin. Yleisesti kyberhyökkääjiä luokitellaan valkohattu-, harmaahattu- ja mustahattuhakkereiksi riippuen toteutettujen kyberhyökkäysten laillisuudesta. Osa kyberhyökkääjistä kuten valkohattuhakkerit on palkattu testaamaan tietoturvaa hyökkäyksillä, kun taas mustahattuhakkerit hyödyntävät tietoturvan haavoittuvuuksia luvattomasti omiin tarkoituksiinsa. (Waschke 2017, 5.) Kyberhyökkääjiä luokitellaan usein myös haktivisteiksi ja kyberterroristeiksi. Hyökkäyksillään haktivistit haluavat tuoda esille omaa viestiään ja usein kohteena ovat erilaiset organisaatiot, jolla on paljon sosiaalista vaikutusvaltaa. Kyberterroristit keskittyvät taas tekemään hyökkäyksiä elämän ja infrastruktuurin kannalta kriittisiin kohteisiin. (Ozkaya 2019, 84.)

Kyberhyökkääjät ovat usein teknisesti osaavia toimijoita, jotka pystyvät hyödyntämään verkkoa ja sen laitteiden ominaisuuksia ja haavoittuvuuksia erittäin taitavasti. Nykyään kyberhyökkääjillä ei kuitenkaan tarvitse olla syvällisempää tietoteknistä tietämystä tai taitoja kyberhyökkäyksien suorittamiseen. Verkko tarjoaa monipuolisesti käyttövalmiita ja tehokkaita työkaluja sekä palveluita, joilla melkein kuka vain voi toteuttaa kyberhyökkäyksen. Taidottomista kyberhyökkääjistä käytetään joskus nimitystä Script kiddie, jolla viitataan usein enemmän nuoriin hakkereihin. Script kiddiet ovat yleensä kykenemättömiä muokkaamaan käyttämiään ohjelmistoja, ja heillä ei ole kattavaa tietämystä käyttämiensä hyökkäysten seurauksista. (Calder 2020, 17-18.) Kyberhyökkääjän ei siis tarvitse olla taidokas hakkeri vaan hyökkääjänä voi toimia myös helposti henkilö, joka on vain utelias ja haluaa kokeilla verkon rajoja.

4 HAITTAOHJELMAT

Haittaohjelmat ovat tietynlaisia tietokoneohjelmia, jotka on suunniteltu aiheuttamaan vahinkoa tietojärjestelmissä tai verkossa käytettävissä laitteissa. Haittaohjelmat esiintyvät yleensä suoritettavan ohjelmakoodin muodossa ja ne leviävät hyödyntäen monipuolisesti eri kanavia verkossa (Monnappa 2018, 6). Haittaohjelmien tarkoituksena on tunkeutua järjestelmiin luvattomasti ja suorittaa omaa ohjelmakoodia toteuttaen haitallisia toimia järjestelmässä (Bijalwan 2022, 36). Suoritetut toiminnot voivat olla datan varastamista, tuhoamista, vakoilua tai luvattoman etähallinnan ja takaovien luomista. Haittaohjelmien avulla pystytään toteuttamaan tehokkaasti monen tyyppisiä hyökkäyksiä ja niitä voidaan käyttää yksittäisesti mutta myös osana toisia kyberhyökkäyksiä. Erilaisia haittaohjelmia luokitellaan usein tiettyihin ryhmiin niiden leviämistekniikan, suoritustavan ja toiminnan perusteella (Bijalwan 2022, 37). Tunnettuja haittaohjelmien luokituksia ovat virukset, madot, troijalaiset, mainos- ja vakoiluohjelmat.

4.1 Virus

Virus on haitallinen ohjelmistokoodi, joka leviää luomalla itsestään kopioita. Virus on yleensä liittynyt ja piiloutunut osaksi toista ohjelmistoa tai tiedostoa. Leviämiseen virus käyttää apunaan sähköpostia ja verkossa jaettavia tiedostoja (Bijalwan 2022, 38). Toimiakseen virus tarvitsee apua verkon käyttäjältä, sillä se ei pysty suorittamaan tehtäväänsä täysin itsenäisesti. Viruksen aktivoituminen tapahtuu siten, että verkon käyttäjä ajaa tartutetun ohjelmiston omalla koneellaan. Onnistuneen suorituksen jälkeen virus pääsee leviämään helposti kaikkiin muihin ohjelmistoihin käyttäjän koneella sekä toisiin laitteisiin samassa verkossa. (Chauhan & Jangra 2020, 13.)

Viruksen päätavoitteena on päästä leviämään mahdollisimman laajalle kopioimalla itseään ja samalla toimittaa omaa ohjelmakoodiaan eteenpäin suoritettavaksi. Virus pyrkii toteuttamaan tämän myös siten, että sen toimintaa ei heti havaittaisi. (Calder 2020,12.) Hyökkääjät pystyvät vaikeuttamaan viruksen havaitsemista ohjelmoimalla niitä tavalla, joka mahdollistaa viruksen muuntautumisen. Virus on yleisesti erittäin tehokas haittaohjelma, koska sen avulla pystytään aiheuttamaan niin pientä kuin suurta vahinkoa tartutetuissa laitteissa. Viruksen tehtävään kuuluu yleensä kopioitumisen ja leviämisen ohella muita toimia kuten sisällön muuttamista tai tuhoamista. Nämä toimenpiteet kohdistuvat usein tartutetun laitteen sisältämiin ohjelmistoihin ja tiedostoihin.

Viruksia voidaan jaotella tiettyihin luokkiin kuten tiedosto-, makro-, käynnistyslohko- ja scripti-virus. Näistä tiedostoviruksella viitataan kaikkiin viruksiin, jotka tartuttavat käyttöjärjestelmän tiedostojärjestelmää. Tämä tekee tiedostoviruksesta yhden suurimmista uhista virusten joukossa, koska niitä käytetään paljon Windowsin käyttöjärjestelmässä, joka hallitsee vahvasti käyttöjärjestelmien markkinoita ja on standardina valtaosalle sovellusohjelmistoista. (Yangchun, Zhao & Yang 2020.) Makrovirus on toinen erittäin yleinen virustyyppi. Tässä viruksessa haitallinen koodi sulautetaan osaksi Microsoft Officen tiedostoa kuten Excel- tai Word-dokumenttia. Tällöin viruksen toiminta saadaan aktiovoitua tartutetun dokumentin avauksen kautta. (Calder 2020, 12.)

4.2 Mato

Mato on haittaohjelma, joka suorittaa omaa ohjelmakoodia itsenäisesti. Mato tartuttaa laitteita pääsääntöisesti sähköpostin ja verkkosivujen välityksellä ja se tarvitsee alussa aktivoituakseen toimia verkon käyttäjältä samoin kuin muut haittaohjelmat. Mato toimii luomalla itsestään kopioita ja leviämällä järjestelmässä automaattisesti hyödyntäen sen haavoittuvuuksia. Tartutetussa laitteessa ja sen järjestelmässä leviämisen lisäksi mato pyrkii leviämään toisiin laitteisiin, jotka ovat samassa lähiverkossa tai muuta kautta yhteydessä tartutettuun laitteeseen. (Johnson 2020.) Levitessään eteenpäin mato ei enää tarvitse erillistä tiedostoa, johon liittyä tai apua verkon käyttäjältä. Kopioituessaan mato vaatii kuitenkin suoran reaaliaikaisen yhteyden kohde ja lähde laitteiden välillä. (Gupta & Goyal 2020, 69.)

Madon toiminnassa yhdistyy piirteitä niin viruksen kuin troijalaisen toiminnasta ja ominaisuuksista (Bijalwan 2022, 38). Madon päätavoitteena on levitä mahdollisimman paljon ja pysyä aktiivisena tartuttamissaan kohteissa. Usein madon tehtävänä on pyrkiä kuluttamaan kaikki resurssit hyökkäyksen kohteeksi joutuneesta laitteesta tai verkosta tehden siitä täysin käyttökelvottoman. Mato onnistuu tässä tehtävässä kopioitumisensa ansiosta. Hyökkäyksessä madon luomien kopioiden määrää kasvaa niin suureksi, että se alkaa hidastaa kohteensa toimintoja huomattavasti ja voi jopa pysäyttää niitä kokonaan. (Chauhan & Jangra 2020, 13.) Resurssien ehdyttämisen lisäksi madolle pystytään antamaan myös muita tehtäviä suoritettavaksi kuten laittomien takaovien avaamista tai toisten haittaohjelmien lisäämistä laitteisiin (Johnson 2020).

4.3 Troijalainen

Troijalainen on haitallista koodia sisältävä ohjelma, joka on piiloutunut tai naamioitu näyttämään viralliselta ja luotettavalta ohjelmistolta. Naamioitumisen ansiosta troijalainen pystyy huijaamaan verkon käyttäjiä lataamaan ja suorittamaan hyökkääjän laatiman ohjelman omalla koneellaan. Troijalainen suunnitellaan näyttämään samalta aidon ohjelmatiedoston kanssa käyttämällä samaa nimeä ja tiedostokokoa kuin oikeassa versiossa (Waschke 2017, 14). Toiminnassaan troijalainen ei hyödynnä itsensä kopiointia, vaan se leviää muihin laitteisiin verkossa tahallisten tiedonsiirtojen mukana (Gupta & Goyal 2020, 69). Leviämiseen troijalainen hyödyntävää erilaisia alustoja kuten nettipelejä, sähköpostia, haitallisia linkkejä ja tiedostoja (McDonough 2019, 48). Kun troijalainen saadaan suoritetuksi onnistuneesti, sillä on mahdollista toteuttaa laaja valikoima erilaisia toimintoja. Vaihtoehdot troijalaisen suorittamalle hyökkäykselle ovat melkein rajattomat erityisesti tilanteissa, joissa troijalainen on suoritettu laitteessa hallinnoitsijan oikeuksilla. (Waschke 2017, 14.)

Troijalaisella asennetaan usein takaovia järjestelmään, jonka avulla saadaan luotua luvaton pääsy laitteelle. Troijalainen muuttaa laitteen asetuksia ja asentaa koodia, jolla takaovi saadaan toimintaan. Takaovien ohella hyökkääjät käyttävät troijalaista varastaakseen ja lähettääkseen uhrin yksityisiä tietoja eteenpäin. Troijalainen pystyy myös tuhoamaan tai kryptaamaan tiedostoja uhrin laitteessa. (Waschke 2017, 14.) Troijalaisen avulla uhrin laitetta on mahdollista käyttää lähteenä kyberhyökkäykselle tai osana muuta laitonta toimintaa. Troijalaisella voidaan vaikuttaa laitteen suojakseen estämällä ja häiritsemällä tärkeitä toimintoja virustentorjuntaohjelmissa tai palomuureissa. Troijalaisella toteutetaan myös keyloggereita, joilla tarkkaillaan ja tallennetaan näppäinsyötteitä.

4.4 Kiristyshaittaohjelma

Kiristyshaittaohjelman tarkoituksena on estää käyttäjän pääsy laitteessa olevaan dataan kuten henkilökohtaisiin tiedostoihin. Kiristyshaittaohjelma tekee datan käyttämisestä lähes mahdotonta kaappaamalla tietoja tai kryptaamalla niitä salattuun ja käyttökelvottomaan muotoon. Näiden lisäksi kiristyshaittaohjelmalla voidaan lukita järjestelmä niin, että sen käyttäminen estyy (Bijalwan 2022, 43). Tietojen haltuun ottamisen jälkeen kiristyshaittaohjelma vaati käyttäjältä lunnaita tietojen palauttamiseksi tai muuttamiseksi takaisin alkuperäiseen muotoon. Lunnaita voidaan vaatia myös tietojen eteenpäin levittämisen ja vuotamisen uhalla. Kiristyshaittaohjelma leviävää verkossa hyödyntäen samoja keinoja

kuin muut haittaohjelmat. Niiden levitys tapahtuu erilaisten latausten ja linkkien kautta. Kiristyshaittaohjelma käyttää myös usein apunaan troijalaisia hyökkäyksen suorittamiseen (Bijalwan 2022, 44).

Kiristyshaittaohjelmien haltuun ottamia tietoja on yleisesti haasteellinen saada takaisin itselleen. Tietoja ei välttämättä saa takaisin edes viranomaisten avustuksella, koska kiristyshaittaohjelmilta puolustautumiseen ei ole panostettu rahallisesti vaan luotetaan enemmän erillisiin tiedostojenpalautustyökaluihin. Palautukseen liittyvien haasteiden seurauksena kiristyshaittaohjelmien uhreiksi joutuneet käyttäjät päätyvät usein maksamaan kiristäjän vaatimia lunnaita tietojen palautuksen toivossa. (McDonough 2019, 45-46.) Vaadittujen lunnaiden määrät vaihtelevasta muutamista satasista useisiin tuhansiin ja maksut halutaan usein suoritettavaksi kryptovaluutoilla (Singh 2020, 16). Lunnaiden maksaminen ei kuitenkaan ole suositeltavaa, sillä kiristyshaittaohjelman takana olevalla hyökkääjällä ei välttämättä ole edes tarvittavia taitoja datan palauttamisen tai muuten aikomusta antaa tietoja takaisin. Lunnaiden maksaminen vaikuttaa myös negatiivisesti hyökkäysten vähentämiseen, koska kiristyshaittaohjelmilla ansaitut varat antavat resursseja uusiin hyökkäyksiin ja kannustavat jatkamaan toimintaa. (McDonough 2019, 45-46.)

4.5 Adware

Adware eli mainosohjelma on haittaohjelma muoto, joka seuraa verkossa käyttäjän mielenkiinnon kohteita ja tuottaa ei-haluttuja mainoksia. Näitä mainoksia näytetään hyökkäyksen kohteeksi joutuneen käyttäjän laitteella. Mainosohjelma avaa mainontaa sisältäviä ponnahdusikkunoita, joita on hyvin haasteellista tai melkein mahdotonta sulkea. Ponnahdusikkunoiden ohella mainosohjelma tekee automaattisia siirtoja sivustojen välillä. Mainosohjelma pystyy uudelleenohjaamaan käyttäjän turvalliselta verkkosivustolta suoraan toiselle haitalliselle sivustolle. (McDonough 2019, 47.) Mainosohjelmat leviävät verkossa käyttäjien koneille helposti erilaisten haitallisten ohjelmisto- ja sovelluslatausten mukana. Suorituksen jälkeen mainosohjelma aloittaa automaattisesti mainosten latauksen ja näyttämisen. (Bijalwan 2022, 39.) Mainosohjelman tavoitteena on yleensä tuottaa rahallista tuloa laatijalleen.

4.6 Spyware

Spyware eli vakoiluohjelma on tarkkailuun ja tietojen keräämiseen suunniteltu haittaohjelma. Vakoiluohjelma tutkii ja kasaa yhteen yksityisiä tietoja hyökkäyksen kohteeksi joutuneesta verkon käyttäjästä ilman hänen suostumustaan. Vakoiluohjelmassa tietojen kerääminen tapahtuu henkilökohtaisten

tiedostojen läpikäymisellä, salasanojen vakoilemisella tai seuraamalla käyttäjää laitteen kameran ja mikrofonin välityksellä (McDonough 2019, 46). Myöhemmin vakoiluohjelma voi välittää hankittuja tietoja eteenpäin toisille järjestelmille ja tahoille (Bijalwan 2022, 43).

4.7 Haittaohjelmien vaikutukset

Monipuolisen haittaohjelma tarjonnan ansiosta haittaohjelmilla on mahdollista toteuttaa paljon erilaisia toimenpiteitä verkossa ja sen laitteissa. Näiden toimien vaikutukset voivat olla vaihetelevia ja ne näkyvät verkon käyttäjälle monella tavalla. Haittaohjelmien aiheuttamilla vaikutuksilla on kuitenkin tiettyjä piirteitä, joita tarkkailemalla käyttäjä pystyy tunnistamaan mahdollisesti laitteellaan olevan haittaohjelman. Haittaohjelmien vaikutukset näkyvät usein laitteessa tapahtuvan epätavallisen toiminnan kautta. Epätavallisena toimintana voidaan pitää sitä, kun käyttäjän oma toiminta laitteella estyy ilman syytä. Käyttäjä ei esimerkiksi pysty avaamaan tarvitsemiaan tiedostoja ja sovelluksia tai laitteen uudelleenkäynnistäminen ei onnistu lainkaan. Epätavalliseen toimintaan voidaan laskea myös se, kun laitteella tapahtuu toimia ilman käyttäjää kuten itsenäisiä osoittimen liikkeitä, tiedostojen latauksia, ohjelmistojen käynnistymisiä tai kameran aktivoitumista.

Haittaohjelmien vaikutukset näkyvät käyttäjälle usein laitteen yllättävänä hidastumisena. Riippuen käytetystä haittaohjelmasta käyttäjän laitteelle voi lisäksi ilmestyä ylimääräisiä ponnahdusikkunoita, mainoksia tai kiristysviestejä. Haittaohjelmat pääsevät myös monesti vaikuttamaan käyttäjien omistamiin tileihin eri palveluissa kuten sähköpostissa ja sosiaalisen median kanavissa. Tällöin käyttäjän yhteystiedoissa oleville henkilölle ilmestyy spämmiä ja huijauksia käyttäjän nimissä. Näiden vaikutusten lisäksi haittaohjelman toiminnan voi tunnistaa tietokoneen työpöydälle ilmestyneistä uusista oudoista kuvakkeista tai selaimen epäilyttävistä työkaluista. (Translated by Content Engine, L.L.C 2022.)

5 PALVELUNESTOHYÖKKÄYKSET

Palvelunestohyökkäys on paljon käytetty kyberhyökkäyksen muoto, jonka tarkoituksena on estää tai muuten lamauttaa tietyn verkkopalvelun tai järjestelmän käyttöä. Palvelunestohyökkäys tunnetaan usein sen englanninkielisellä termillä DoS, joka tarkoittaa Denial of Service eli palvelun estämistä. Palvelunestohyökkäys toteutetaan lähettämällä verkossa erilaisia pyyntöjä toimintojen toteuttamiseksi halutussa kohteessa. Hyökkäyksessä lähetettyjen pyyntöjen määrä on erittäin suuri ja niitä lähetetään yhtäjaksoisesti nopealla tahdilla. Tämän tarkoituksena on ylikuormittaa kohteena olevaa verkon palvelua, järjestelmää tai sivustoa mahdollisimman paljon. Ylikuormittumisen seurauksena kohteen toiminta hidastuu merkittävästi tai se kaatuu kokonaan, jolloin se ei ole enää virallisten käyttäjien saatavilla. Tämän tyyppiset tulvat ovat erittäin suosittu ja yksinkertainen tapa palvelunestohyökkäysten suorittamiseen. Kyberhyökkääjällä on kuitenkin käytössään myös muita tekniikoita hyökkäyksen toteuttamiseen. Näitä ovat palvelun uudelleenohjaus, korvaaminen tai poistaminen. (Chauhan & Jangra 2020, 115.)

Palvelunestohyökkäyksestä käytetään usein myös toista termiä DDoS eli Distributed Denial of Service, jolla tarkoitetaan hajautettua palvelunestohyökkäystä. Palvelunestohyökkäyksen sanotaan olevan hajautettu silloin, kun hyökkäyksessä käytetyt toiminnot ja pyynnöt tulevat kohteeseen samanaikaisesti suuresta määrästä eri laitteita. Nämä useiden laitteiden verkostot on usein toteutettu hyödyntämällä bottiverkkoja. Kyberhyökkääjät suosivat hajautettua palvelunestohyökkäystä yksittäisen palvelunestohyökkäyksen sijaan, koska niillä hyökkäyksestä saadaan entistä tehokkaampi. Hajautetussa palvelunestohyökkäyksessä myös kiinni jäämisen riski pienenee, koska hyökkäyksen alkuperäistä lähdettä on haasteellisempi jäljittää. Palvelunestohyökkäyksen kohteeksi valikoituvat yleisesti korkeamman luokan verkkopalvelut ja -sivustot kuten pankit tai valtiolliset palvelut (Gupta & Goyal 2020, 52, 56.)

5.1 Bottiverkko

Bottiverkoksi kutsutaan verkostoa, joka koostuu suuresta määrästä kyberhyökkääjän haltuun ottamia tietokoneita tai muita verkossa toimivia laitteita. Bottiverkkoja käytetään paljon hajautettujen palvelunestohyökkäysten toteuttamiseen. Niitä hyödynnetään kuitenkin myös muuhun haitalliseen toimintaan kuten spämmin ja virusten levitykseen. (Bijalwan 2022, 203). Yksittäinen bottiverkko voi koostua, jopa sadoista tai tuhansista verkon laitteista (Brooks, Grow, Craig & Short 2018, 607). Bottiverkon muodostavista yksittäisistä laitteista käytetään nimitystä botti tai zombi. Botit ovat yksityisten

käyttäjien omistamia laitteita, joihin hyökkääjä on saanut luvattoman pääsyn haitallisen ohjelmakoodin avulla. Laitteen joutuminen osaksi bottiverkkoa tapahtuu usein virallisten käyttäjien tietämättä. Tapahtumana havaitseminen on usein vaikeaa, koska laitteessa luvattoman käytön vaikutukset näkyvät vain ajoittain, kun botti on aktiivisesti käytössä. (Waschke 2017, 20.)

Bottiverkkoa hallitseva kyberhyökkääjä eli botmaster toteuttaa hyökkäyksiä antamalla laitteille käskyjä, joita niiden tulee suorittaa. Annettujen käskyjen taso vaihtelee bottiverkon ominaisuuksien mukaan. Osa bottiverkoista voi toteuttaa vain yksinkertaisia käskyjä mutta monimutkaisten ohjelmien suorittaminen on myös mahdollista. (Waschke 2017, 20.) Yleisesti kyberhyökkääjällä on monia eri keinoja oman bottiverkkonsa rakentamiseen, mutta usein laitteet verkostoon saadaan troijalaisten avulla. Nykyään kuitenkin bottiverkon muodostamiseksi hyökkääjällä ei välttämättä tarvitse olla paljon osaamista, sillä verkossa on saatavilla palveluita, jotka tarjoavat valmiita bottiverkkoja. (Brooks ym. 2018, 607.)

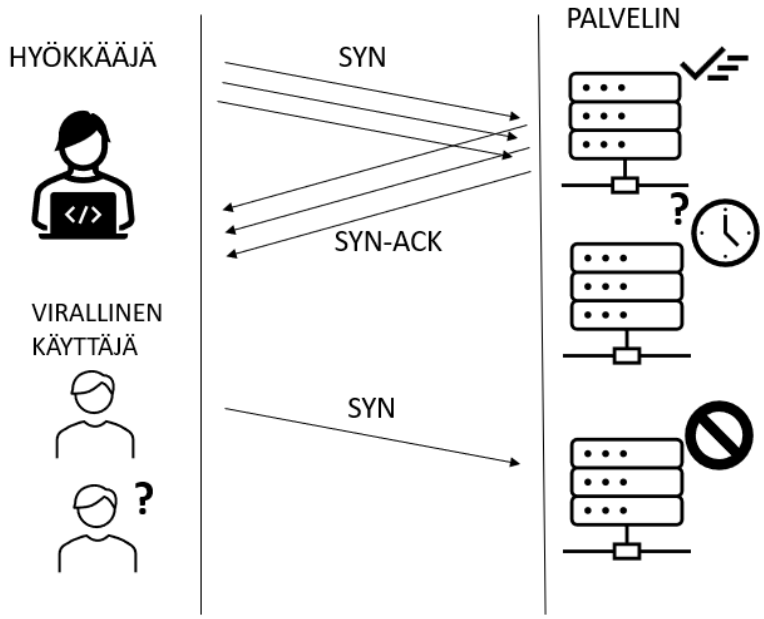
5.2 Tulvahyökkäykset

Tulvahyökkäyksillä tarkoitetaan yleisesti palvelunestohyökkäyksiä, joissa käytetään ja lähetetään suuri määrä verkon paketteja. Paketit voivat olla verkon istuntoon liittyviä yhteyspyyntöjä tai muun tyyppisiä pyyntöjä. Tulvahyökkäyksissä käytettyjen pyyntöjen muoto vaihtelee sen perusteella, mihin verkkokerroksista hyökkäyksellä halutaan vaikuttaa. Pyynnöt hyväksikäyttävät monipuolisesti verkon eri protokollia ja niiden ominaisuuksista löytyviä haavoittuvuuksia. Yleisiä tulvahyökkäyksen tyyppejä ovat TCP-, SYN-, UDP-, ICMP- ja HTTP-tulvat. Näistä tulvahyökkäyksistä UDP-, ICMP- ja HTTP-tulvaa käytetään enimmäkseen kaistanleveyden kuluttamiseen. Muissa tulvahyökkäyksissä kuluttaminen kohdistuu pääasiassa erilaisten resurssien ehdyttämiseen. (Bijalwan 2022, 45.)

5.2.1 SYN-tulva

SYN-tulva on helppo ja yleinen tulvahyökkäyksen muoto, joka hyödyntää TCP-protokollan sisältämiä haavoittuvuuksia. SYN-paketteja käytetään TCP-protokollan kolmivaiheisessa kättelyssä, jonka tarkoituksena on varmistaa lähetetyn datan eheys yhteyden aikana. (Bijalwan 2022, 45.) SYN-tulvassa hyökkääjä lähettää valheellisilla lähetysosoitteilla varustettuja SYN-paketteja palvelimelle. Nämä lähetetyt paketit tulkitaan pyynnöksi yhteyden muodostamiselle, jonka seurauksena palvelin avaa osittaisen

yhteyden. Samalla palvelin vastaa lähettäjälle yhteyden hyväksynnästä kertovalla TCP/SYN-ACK-paketilla. Palvelin jää odottamaan pakettiin vastausta alkuperäiseltä lähettäjältä, mutta sitä ei koskaan tule. Palvelimella odottavat yhteydet kuluttavat palvelimen kapasiteettia tarjota yhteyksiä, jolloin se ei pysty vastaanottamaan pyyntöjä virallisilta käyttäjiltä. (Gupta & Goyal 2020, 53.) (KUVA 1.)

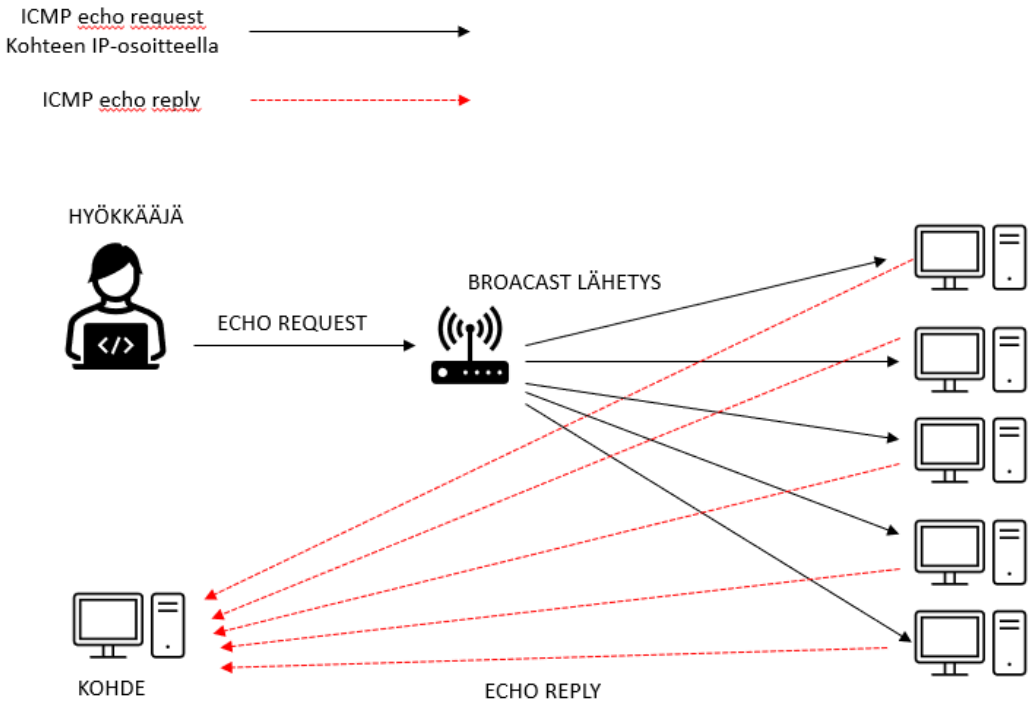


KUVA 1. SYN-tulvan toimintaperiaate (mukaillen Dake, 2006)

5.2.2 ICMP-tulva

ICMP-tulva on tulvahyökkäys, jonka tarkoituksena on kuluttaa kaistanleveyttä. ICMP-protokollaa käytetään yleisesti yhteyksien tarkistamiseen, jotta voidaan varmistua siitä, että kohde verkossa on olemassa ja tavoitettavissa. ICMP-tulvassa kohdeverkko kyllästetään lähettämällä sinne valtavasti ICMP-paketteja. Tällöin kyseisen verkon on mahdotonta prosessoida vastaanottamiaan paketteja normaalisti, jolloin verkkoliikenne muuttuu niin, että viralliset käyttäjät eivät saa enää yhteyttä verkkoon. (Bijalwan 2022, 46.) ICMP-tulva on mahdollista toteuttaa eri tavoilla kuten käyttämällä ping-komennon echo request -pyyntöä. ICMP-tulvaa voidaan myös hyödyntää osana smurf-hyökkäyksiä, jotka pohjautuvat virheellisesti konfiguroituihin verkkolaitteisiin. Näissä laitteissa pakettien lähetys on sallittu broadcast-osoitteella kaikille laitteille tietyssä verkossa yksittäisen laitteen sijaan. Smurf-hyökkäyksessä suuri määrä ICMP-paketteja lähetetään broadcast-osoitteelle väärennetyllä lähde IP-osoitteella,

joka kuuluu hyökättävälle kohteelle. Tällöin kaikki takaisin tulevat vastaukset kohdistuvat väärennettyyn osoitteen, mikä kuluttaa saatavilla olevan verkon kaistanleveyden kokonaan. (KUVA 2.) Kaistanleveyden nopea kulumien estää muilta verkon käytön, kun viralliset verkkopaketit eivät pääse läpi omaan kohteeseensa. (Gupta & Goyal 2020, 52-53.)



KUVA 2. ICMP-tulvalla toteutettu smurf-hyökkäys (mukaillen Imperva Incapsula 2014)

6 MUITA YLEISIÄ KYBERHYÖKKÄYKSIÄ

Nykypäivän globaali ja monimuotoinen verkkoympäristö tarjoaa valtavasti hyviä ominaisuuksia ja palveluita käyttäjilleen, mutta myös paljon mahdollisuuksia erilaisille kyberhyökkäyksille. Erityyppiset haittaohjelmat ja palvelunestohyökkäykset kattavat vain osan näistä vaihtoehdoista. Mainittujen kategorioiden ulkopuolelle jää vielä paljon muita kyberhyökkäyksen muotoja, jotka hyödyntävät verkkoa ja sen haavoittuvuuksia eri tavoilla. Muita yleisiä kyberhyökkäyksiä ovat esimerkiksi Man-in-the-Middle, Zero-Day, phishing, injektiohyökkäykset ja salasanoihin kohdistuvat hyökkäykset.

6.1 Zero day -haavoittuvuus ja -hyökkäys

Zero day -hyökkäykseksi kutsutaan kyberhyökkäystä, joka hyödyntää verkon järjestelmässä, laitteessa tai palvelussa esiintyvää Zero day -haavoittuvuutta. Haavoittuvuuden sanotaan olevan Zero day -haavoittuvuus silloin, kun sitä ei ole vielä saatu palvelun tarjoajan tai tuottajan tietoisuuteen. Tällöin haavoittuvuuden korjaustoimenpiteitä ei ole vielä aloitettu ja virallista paikkausta ei ole saatavilla. (Waschke 2017, 16.) Hyökkääjät etsivät mielellään zero day -haavoittuvuuksia, koska niiden avulla toteutetut zero day-hyökkäykset ovat helppoja ja tehokkaita. Lisäksi zero day -hyökkäysten todennäköisyys onnistua on todella hyvä, mikä tekee niistä entistä suositumpia kyberhyökkääjien keskuudessa (Calder 2020, 17).

Zero day -haavoittuvuudet ovat hyökkäysten tehtailun ohella hyökkääjälle arvokasta kauppatavaraa, ja niille on olemassa oma pimeän kaupan markkina. Kyberhyökkääjät pystyvät tienaamaan jopa useita tuhansia löytämiensä Zero day -haavoittuvuuksien avulla. Monilla rikollisorganisaatiolla ja valtion tahoilla on kerättynä varastoon useita zero day -haavoittuvuuksia odottamaan hetkeä, jolloin zero day -hyökkäysten käyttöä tarvitaan. (Waschke 2017, 16.) Yleisesti zero day -hyökkäykset ovat erittäin haitallisia ja toimivia kyberhyökkäyksiä, koska kukaan tai mikään ei ole niiltä täysin suojassa. Zero day -hyökkäyksiä on mahdollista tehdä onnistuneesti myös täysin paikattuja ja moderneja järjestelmiä ja laitteita vastaan. (Donaldson, Williams & Siegel 2018, 24.)

6.2 Phishing

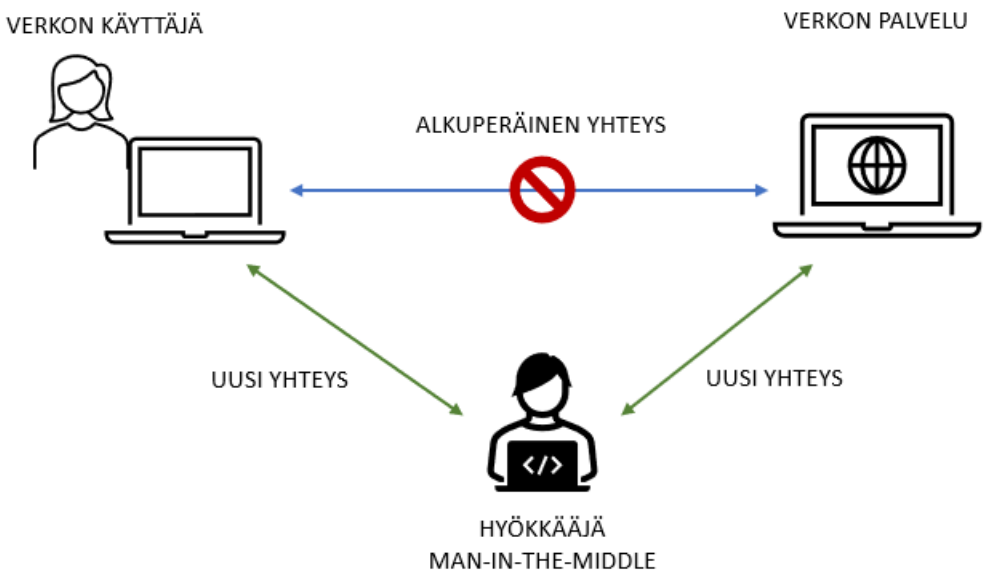
Phishing on tietojenkalasteluun käytetty kyberhyökkäys, jonka tarkoituksena on saada verkon käyttäjää luovuttamaan henkilökohtaisia ja arvokkaita tietoja hyökkääjälle. Phishigissä hyökkääjä houkuttelee kohteen antamaan omia tietojaan eteenpäin käyttämällä syöttiä kuten sähköpostia tai muuta viestiä. Käytetty syötti vaikuttaa tulevan viralliselta tai muuten luotettavalta lähteeltä. Phishingiä toteutetaan yleensä juuri sähköposteilla, mutta sen toteutuksessa voidaan hyödyntää myös spämmiä tai muuta kohteelle suoraan kohdennettua sisältöä. Hyökkäyksessä käytetyt sähköpostit sisältävät usein tartutettuja ja haitallisia ohjelmistoja, dokumentteja ja linkkejä. (Donaldson ym. 2018, 16.) Näiden lisäksi phishing-viesteissä esiintyy valheellisia sosiaalisen median pyyntöjä, ilmaisia tuotetarjouksia, ilmoituksia palkinnon voittamisesta ja tilauksiin liittyviä ilmoituksia. Phishingissä hyödynnetään myös paljon taktiikoita, joilla hyökkäyksessä esitetty asia saadaan tuntumaan kriittiseltä ja nopeasti hoidettavalta. Phishingiä on mahdollista toteuttaa monipuolisesti ja se onkin yksi yleisimmistä tavoista, joilla verkon käyttäjä joutuu hakkeroinnin kohteeksi. (McDonough 2019, 33-35.)

6.3 Man-in-the-Middle

Man-in-the-middle on hyökkäys, jossa hyökkääjä on osallisena virallisten käyttäjien välisessä kommunikaatiossa ja verkkoliikenteessä heidän tiedostamattaan. Man-in-the-middle-hyökkäyksessä yksityiseksi tarkoitettua verkkoliikennettä voidaan tarkkailla, muokata, varastaa ja käsitellä muilla tavoin hyökkääjän toimesta. Man-in-the-middle-hyökkäys on mahdollista suorittaa onnisteneesti hyödyntämällä monia eri tekniikoita. Yksinkertaisesti man-in-the-middle-hyökkäys on voitu toteuttaa luomalla epävirallinen ilmainen Wi-Fi-jakopiste julkiselle paikalle kuten kahvilaan. Käyttäjien yhdistyessä tähän verkkoon hyökkääjä pääsee tarkkailemaan siellä liikkuvaa verkkoliikennettä ja keräämään itselleen arvokkaita tietoja. (Waschke 2017, 14.) Näiden valheellisten verkkojen lisäksi hyökkääjät voivat häiritä myös virallisia verkkoja suorittaessaan man-in-the-middle-hyökkäystä. Hyödyntäessään verkkoliikennettä hyökkääjä pyrkii poistamaan siitä kaikki kryptaukset saadakseen sen sisältämän tiedon selkokieliseen muotoon, jolloin sitä on mahdollista käsitellä. (Swinhoe 2019.)

Toinen mahdollinen tapa man-in-the-middle-hyökkäyksen suorittamiseen on luoda väärennetty versio käyttäjän tavoittelemasta verkkosivustosta. Tällöin sivustolle syötetyt tiedot siirtyvät suoraan hyökkääjälle, joka voi muuttaa niiden sisältöä haluamallaan tavalla. Sisällön muuttamisen jälkeen hyökkääjä toimittaa tiedot eteenpäin viralliselle kohteelle väärällä lähde-IP-osoitteella. Näin kohteelta palautuva

vastaus saadaan ohjattua suoraan hyökkääjälle, jolloin sen sisältöä voidaan käsitellä taas ennen lähetystä alkuperäiselle käyttäjälle. (KUVA 3.) Verkkoliikenteeseen vaikuttamisen lisäksi man-in-the-middle-hyökkäyksiä pystytään käyttämään monipuolisesti eri käyttötarkoituksiin kuten tietojen varastamiseen tai haittaohjelmien syöttämiseen käyttäjien laitteille. (Waschke 2017, 13-14.) Yleisesti Man-in-the-middle-hyökkäysten havaitseminen on verkon käyttäjille erittäin haasteellista, koska verkkoliikenne saadaan vaikuttamaan lähes normaalilta hyökkäyksen aikana.



KUVA 3. Man-in-the-middle-hyökkäyksen toimintaperiaate (mukaillen Nasanbuyn 2016)

6.4 Injektiohyökkäykset

Injektiohyökkäys on kyberhyökkäyksen muoto, joka on toteutettu epäluotettavien ohjelmistosyötteiden avulla. Injektiohyökkäyksessä hyökkääjä kirjoittaa ohjelmistolle epävirallisen syötteen, joka käsitellään normaalin komennon tai kyselyn mukaisesti ohjelmistotulkin toimesta. Tämän ansiosta hyökkääjä pääse vaikuttamaan ohjelmiston toimintaan ja muuttamaan sitä haluamallaan tavalla. Injektiohyökkäykset kattavat laajan skaalan erilaisia injektioita, joilla hyökkäys voidaan suorittaa. Näistä yleisimpiä ovat käyttöjärjestelmä komennot, SQL-, ORM-, LDAP-, ja OGNL-injektiot. (Singh 2020, 34.) Injektiohyökkäykset toimivat erittäin tehokkaasti silloin, kun virallinen ohjelmisto tai sivusto ei pysty tekemään eroa käyttäjältä tulevan syötteen ja aidon ohjelmistokomennon välillä.

6.4.1 SQL-injektio

SQL-injektio on yleinen injektiohyökkäys, jonka tarkoituksena on päästä vaikuttamaan erilaisiin tietokantoihin verkkosivustojen tai muiden verkon sovellusten kautta. SQL-injektiossa hyökkääjä suorittaa haitallisia SQL-kyselyjä heikosti konfiguroiduissa verkon sovelluksissa. (Ozkaya 2019, 15). Injektiossa SQL-komennolla laadittu kysely lisätään sivuston tai sovelluksen julkiseen syötteitä vastaanottavaan kenttään kuten kirjautumislomakkeeseen. Tätä kautta hyökkääjä saa pääsyn sovelluksen tai sivuston taustalla toimivaan tietokantaan ja sen sisältämään dataan. (Brooks ym. 2018, 594.) Onnistunut pääsy tietokantaa avaa hyökkääjälle mahdollisuuden arkaluontoisen datan manipulointiin ja muokkaamiseen (Ozkaya 2019, 15).

6.4.2 Cross-site scripting

Cross-site scripting on injektiohyökkäys, joka tunnetaan lyhyemmin nimellä XSS. Cross-site scriptingissä hyökkääjä käyttää hyväkseen verkkosovellusten ja -sivustojen haavoittuvuuksia. Nämä haavoittuvuudet mahdollistavat haitallisen ohjelmakoodin syöttämisen sivuston käyttäjäpuolelle. (Ozkaya 2019, 14.) Sivustolle syötetty ohjelmakoodi lisätään usein verkkosivun sisältämiin lomakekenttiin tai URL-syöttökenttään. XSS-hyökkäyksessä käytetty ohjelmakoodi on yleensä toteutettu JavaScript ja HTML-kielien avulla. XSS-hyökkäyksessä haitallinen koodi on asetettu sivustolle niin, että se saa pääsyn uhrin tietokoneelle, kun kyseistä sivustoa käytetään. (Fruhlinger 2022.) Näin sivustolla oleva haitallinen ohjelmakoodi saadaan suoritetuksi virallisen käyttäjän selaimessa hänen tiedostamattaan. Tämän on mahdollista sen takia, että selain on kykenemätön erottamaan haitallista ohjelmakoodia virallisen sisällön joukosta. Onnistuneen XSS-hyökkäyksen avulla hyökkääjä voi suorittaa paljon erilaisia toimia kuten kaapata istuntoja, varastaa evästeitä, levittää haittaohjelmia, manipuloida verkkosisältö tai uudelleenohjata haitallisille sivustoille. (Sarmah, Bhattacharyya & Kalita 2018.)

XSS-hyökkäyksestä on kolme eri kategoriaa, joihin se jaotellaan käytetyn ohjelmakoodin toimitus- ja suoritustapojen perusteella. Nämä kategoriat ovat tallennettu, heijastettu ja DOM-pohjainen XSS-hyökkäys, joista heijastettu on kaikista yleisin. Heijastetussa XSS-hyökkäyksessä hyökkääjä tyypillisesti lähettää käyttäjälle muunnellun linkin ja houkuttelee painamaan sitä. Linkki painamisen seurauksena palvelimelle lähetetään kysely, johon palvelin heijastaa vastauksena haitallista koodia. Koodi tulee suoritetuksi käyttäjän selaimessa automaattisesti palvelimelta vastaanottamisen jälkeen. (KUVA 4.)

Tallennetussa XSS-hyökkäyksessä haitallinen ohjelmakoodi tallennetaan pysyvästi sivuston palvelimelle. Tallennus palvelimelle tapahtuu esimerkiksi viesti foorumien, blogi postausten tai kommenttien kautta. Käyttäjän selain suorittaa tallennetun koodin sivustolla vierailemisen yhteydessä. (Sarmah ym. 2018.)

KUVA 4. Heijastetun Cross-site scripting hyökkäyksen toimintaperiaate. (mukaillen Sharmah ym. 2018)

DOM-pohjainen XSS-hyökkäys eroaa heijastetusta ja tallennetusta hyökkäyksestä, koska siinä hyödynnetään käyttäjän selaimen haavoittuvuuksia palvelimen haavoittuvuuksien sijaan. DOM-pohjaisessa XSS-hyökkäyksessä sivuston DOM-objekteja ja HTML ominaisuuksia käsitellään niin, että haitallisen ohjelmakoodin suorittaminen onnistuu. DOM-pohjaisia hyökkäyksiä toteutetaan yleensä muunnellun URL:n avulla niin, että hyökkäyksen käyttämä sisältö on osana verkkosivun DOM:ia. Tällöin hyökkäyksen sisältö ei tule osaksi palvelimen toimintoja. Useissa tapauksissa DOM-pohjaisten hyökkäysten haitallinen koodi ei edes tavoita palvelinta. (Sarmah ym. 2018.)

6.5 Salasanahyökkäykset

Salasanahyökkäys on kyberhyökkäyksen muoto, joka kohdistuu erityisesti verkon käyttäjien salasanoihin. Hyökkäyksen pääasiallisena tarkoituksena on päästä käyttämään salasanoja luvattomasti niiden murtamisen kautta. Salasanat ovat erittäin arvokas kohde hyökkääjille, koska ne toimivat avainasemassa niin verkon turvallisuuden luomisessa kuin käyttäjän yksityisyyden suojelemisessa. Nykyään salasanat ovat yksi tärkeimmistä ja käytetyimmistä todennuksen keinoista verkossa, mikä tekee niistä houkuttelevan kohteen hyökkäyksille. Salasanojen murtaminen on erittäin yleistä ja sitä toteutetaan

paljon sen hyödyllisyyden ja tehokkuuden takia. Onnistunut salasanahyökkäys antaa hyökkääjälle suuren edun avaamalla mahdollisuuksia erilaisille haitallisille toimille kuten käyttäjien tilien väärinkäytölle ja arkaluontoisten tietojen laittomalle käsittelylle.

Salasanahyökkäyksissä salasanojen murtamiseen käytetään paljon kahta tekniikkaa, jotka ovat brute force ja sanakirjahyökkäys. Brute forcessa eli raa'an voiman tekniikassa salasana murrettaan testaamalla kaikki mahdolliset salasana vaihtoehdot läpi, kunnes oikea löytyy. Salasanan pituus ja monimutkaisuus vaikuttaa siihen, kuinka paljon salasanan löytäminen vie aikaa ja kuinka haasteellista tekniikkaa on toteuttaa. Brute force toimii parhaiten, kun käytössä on vain pieni määrä salasanavaihtoehtoja. (Jian 2022.) Läpi käytävien salasanojen vaihtoehdot vähenevät, kun salasanassa käytetään helposti murrettavia yhdistelmiä kuten pelkkiä numeroita, kirjaimia tai molempia yhdessä. Brute force -tekniikka on hyvin yksinkertaista ja nopeaa toteuttaa käyttämällä siihen tarkoitettuja ohjelmakoodeja.

Salasanahyökkäyksissä toinen käytetty tekniikka on sanakirjahyökkäys, joka on kehittyneempi muoto brute forcesta. Sanakirjahyökkäyksessä oikea salasana pyritään murtamaan löytämällä sen pari tietystä sanakirjatiedostosta. (Jia 2022.) Sanakirjan ansiosta mahdollisten vaihtoehtojen määrää salasanoissa saadaan rajattua paljon alkuperäistä pienemmäksi (Waschke 2017, 17). Sanakirjatiedostot koostetaan yleensä sanoista, joita esiintyy usein salasanoina. Sanakirjatiedostot voivat perustua myös tiettyihin merkkijonosetteihin tai aitoihin salasanasetteihin, joita on vuotanut ulkopuolisille. (Jia 2022.) Brute force -tekniikoiden ohella salasanahyökkäyksiin pystytään käyttämään monia muita metodeja. Näissä metodeissa voidaan hyödyntää troijalaisia, verkkoliikenteen tarkkailua tai IP-osoitteiden väärentämistä. (Chauhan & Jangra 2020, 149.)

7 KYBERHYÖKKÄYSTEN TORJUMINEN

Tiedon lisääminen kyberhyökkäyksistä ja niiden toiminnasta on hyödyllistä jokaiselle verkon käyttäjälle. Kattavalla perustiedolla verkon käyttäjän on helpompi havaita ja tunnistaa verkossa tapahtumia, jotka viittaavat erilaisiin kyberhyökkäyksiin. Opitut tiedot auttavat käyttäjää tarkastelemaan verkon sisältöjä, palveluita ja verkkoon liitettyjen laitteiden toimintaa aikaisempaa kriittisemmin. Verkossa tarkkaavaisella ja analysoivalla toiminnalla käyttäjän on mahdollista välttää monia kyberhyökkäyksistä. Ymmärrys hyökkäyksistä helpottaa myös niiden torjuntaa, kun tiedetään, minkälaisia uhkia meihin kohdistuu. Torjunnan kannalta erilaisten kyberhyökkäysten tunnistaminen on yleisesti tärkeää, mutta sillä ei yksistään pystytä takaamaan hyvää kyberturvallisuutta. Tehokas kyberhyökkäysten torjunta vaatii usein rinnalleen muita puolustusta vahvistavia toimenpiteitä ja ohjelmistoja.

Nykyään toimivaa kyberhyökkäysten torjuntaa varten on onneksi tarjolla monia eri ratkaisuja kuten esimerkiksi virustorjuntaohjelmat, palomuurit ja hyvät salasana käytännöt. Monipuolisista torjunta keinosta huolimatta kyberturvallisuudesta ei kuitenkaan löydy sellaista ratkaisua, jolla voitaisiin tarjota täydellistä suojaa kaikkia uhkia vastaan. Teknologian kehittyminen antaa hyökkääjille aina uusia tapoja ja työkaluja, joilla voidaan suorittaa entistä monimutkaisempia kyberhyökkäyksiä. Verkon käyttäjät voivat kuitenkin pienentää tulevaa vahinkoa ottamalla käyttöön teknologioita, joilla kyberhyökkäysten täsmällinen tunnistus on mahdollista ajoissa. Hyökkäyskierteen pysäyttäminen sen alkuvaiheessa auttaa käyttäjää välttymään monilta hyökkäyksestä aiheutuvilta harmeilta. (Singh 2020, 135-136.) Kokonaisuudessaan kyberhyökkäysten torjunta onnistuu parhaiten silloin, kun torjunnassa otetaan käyttöön useampi turvatoimi yhtä aikaan. Tällöin kyberhyökkäysten torjunnasta luodaan kattava ja vahva kokonaisuus, jossa ohjelmistot ja tekniikat täydentävät toistensa puutteita.

7.1 Yleisiä toimintatapoja kyberhyökkäysten torjumiseen

Toimiva kyberhyökkäysten torjunta on mahdollista aloittaa yksinkertaisten tekojen kautta. Tarkkaavaisella asenteella ja kyberhyökkäysten toiminnan tiedostamisella onnistutaan torjumaan jo paljon hyökkäyksiä. Omien toimintamallien ohella kyberhyökkäysten torjuntaa on järkevää lähteä kehittämään laitteiden kautta, koska ne sisältävät suuren määrän arvokasta dataa käyttäjistään. Verkon käyttäjät pystyvät helposti vahvistamaan käyttämiensä tietokoneiden ja mobiililaitteiden valmiutta torjua ky-

berhyökkäyksiä. Tämä onnistuu käyttämällä uusimpia versioita käyttöjärjestelmistä ja laitteen sisältämistä ohjelmistoista. Käyttöjärjestelmän ja ohjelmistojen ajoittainen päivittäminen on myös tärkeää, koska sen avulla hyökkäyksille altistavia haavoittuvuuksia saadaan korjattua. Laitteilla olevien käyttämättömien ja vanhojen ohjelmistojen poistaminen on myös järkevää, sillä suuri ohjelmistojen määrä luo aina enemmän mahdollisuuksia haavoittuvuuksille. (Donaldson ym. 2018, 24-25.)

Ohjelmistojen ja käyttöjärjestelmien ylläpidon ohella käyttäjän kannattaa erikseen suojata laitteissa olevia yksityisiä ja arvokkaita tiedostoja. Ennakoivat toimenpiteet datan suojaamisessa ovat tehokas tapa torjua kyberhyökkäysten vaikutuksia ja varmistaa tietojen palauttaminen tarvittaessa. Datan suojaamiseksi käyttäjän kannattaa aloittaa säännöllinen varmuuskopiointi laitteen tärkeille tiedostoille. Varmuuskopiointi voidaan toteuttaa tallentamalla kopioita tärkeästä datasta pilvipalveluihin tai ulkoisiin tallennustiloihin kuten erilliselle kovalevylle. Varmuuskopioinnin lisäksi tiedostojen kryptaaminen paikallisesti laitteessa sekä pilvipalveluissa suojaa dataa kyberhyökkäyksiltä. Tiedostojen kryptaamisen voi toteuttaa käyttämällä tietokoneen sisäänrakennettuja työkaluja tai muun luotettavan tahon tarjoamia ratkaisuja. (McDonough 2019, 165-166.)

Ohjelmistojen ja datan suojaamisen lisäksi verkon käyttäjän on hyvä kiinnittää huomiota siihen, että verkon selaaminen ja latausten tekeminen olisi mahdollisimman turvallista. Näin käyttäjät pystyvät pienentämään kyberhyökkäysten kohteeksi joutumisen riskiä. Verkkoa selatessaan käyttäjän tulisi muistaa tarkistaa, että palveluissa käytetyt yhteydet ovat turvallisia. Käyttäjä voi varmistaa turvallisen yhteyden sivustoilla tutkimalla verkon osoitekenttää. Osoitekentässä näkyvä lukkokuvake ja osoitteen aloittava https:// -merkintä kertovat käytetyn yhteyden turvallisuudesta. Klikattujen linkkien, mainosten ja sivustojen suhteen tulisi olla myös tarkkaavaisena, jottei niiden kautta vahingossa ajaudu epäluotettaville sivustoille. Verkkosivustoissa kannattaa kiinnittää huomiota erilaisiin kirjoitusvirheisiin niiden osoitteissa, koska ne voivat viestiä väärennetyistä sivustoista. Verkossa tulisi myös välttää ilmaisen sisällön kuten elokuvien, musiikin tai ohjelmisto kopioiden etsimistä, koska ne johtavat usein epäluotettaville sivustoille. (Donaldson ym. 2018, 67-69.)

Verkkolataukset ja niiden hallinta on erittäin oleellista kyberhyökkäysten torjunnan kannalta, koska useimmat hyökkäyksistä hyödyntävät juuri lautauksia itsensä levittämiseen ja oman toimintansa aloittamiseen. Verkon käyttäjän on mahdollista ennaltaehkäistä erilaisia kyberhyökkäyksiä varmistamalla, että lataukset tehdään luotettavista ja alkuperäisistä lähteistä. Erilaisia ohjelmistoja ladatessa olisi hyvä

käyttää niiden valmistajien sivustoja tai virallisia sovelluskauppoja. Tiedostojen ja ohjelmistojen skannaaminen virustorjuntaohjelmistolla niiden latauksen ja asennuksen aikana on myös suositeltavaa, jotta latausten sisällön aitous voidaan tarkistaa. (Donaldson ym. 2018, 73.)

7.2 Virustorjuntaohjelma

Virustorjuntaohjelmaksi kutsutaan ohjelmistoa, joka on suunniteltu havaitsemaan ja estämään erilaisia haittaohjelmia. Nykyään monissa tietokoneissa virustentorjuntaohjelma on valmiiksi asennettu ja se kuuluu osaksi käyttöjärjestelmän omia puolustus ominaisuuksia. Virustorjuntaohjelmana voidaan kuitenkin käyttää myös jonkun muun ulkoisen tietoturvallisuus yrityksen tarjoamaa maksullista ohjelmistoa. Normaalisti virustorjuntaohjelmalla on käytössään monipuolisesti turvallisuutta vahvistavia ominaisuuksia. Tämän ansiosta sillä voidaan tarjota käyttäjälle tehokasta suojausta liittyen laitteisiin, dataan ja verkon käyttöön.

Virustorjuntaohjelman yleinen ominaisuus on kyky havaita ja tunnistaa ennestään tunnettuja haittaohjelmia. Lisäksi virustorjuntaohjelma kykenee tunnistamaan kyberhyökkäysten toimintaan viittaavia merkkejä laitteen ohjelmistoissa ja järjestelmässä. Virustorjuntaohjelmalla on mahdollista parantamaan käyttäjän yksityisyyttä suojaamalla salasanoja, käyttäjätietoja ja maksutietoja verkossa. Näiden tietojen ohella virustorjuntaohjelma suojaa ja salaa itse laitteella olevaa dataa. Virustentorjuntaohjelmalla voidaan myös vahvistaa verkon selauksen ja sähköpostin käytön turvallisuutta. Lisäksi moni virustorjuntaohjelma mahdollistaa verkossa tehtyjen latausten tarkastamisen skannaamalla ne haittaohjelmien varalta. Virustorjuntaohjelman tarjoamiin suojaus ominaisuuksiin on hyvä tutustua, koska kaikki ohjelmistot eivät sisällä täysin samoja ominaisuuksia. Usein kolmannelta osapuolelta hankitut virustorjuntaohjelmat tarjoavat kattavamman valikoiman turvallisuus ominaisuuksia. (Donaldson ym. 2018, 26.)

7.3 Palomuuri

Palomuuri on laite tai ohjelmisto, jonka on suunniteltu estämään verkossa tapahtuvia hyökkäyksiä suodattamalla ja kontrolloimalla verkkoliikennettä. Palomuuri asetetaan sisäisen ja ulkoisen verkon välille, jolloin se pystyy käsittelemään lähtevään ja tulevaan verkkoliikennettä ja sen paketteja. Palomuurien yhteydessä sisäisellä verkolla viitataan yleensä luotettuun paikalliseen verkkoon ja sen laitteisiin,

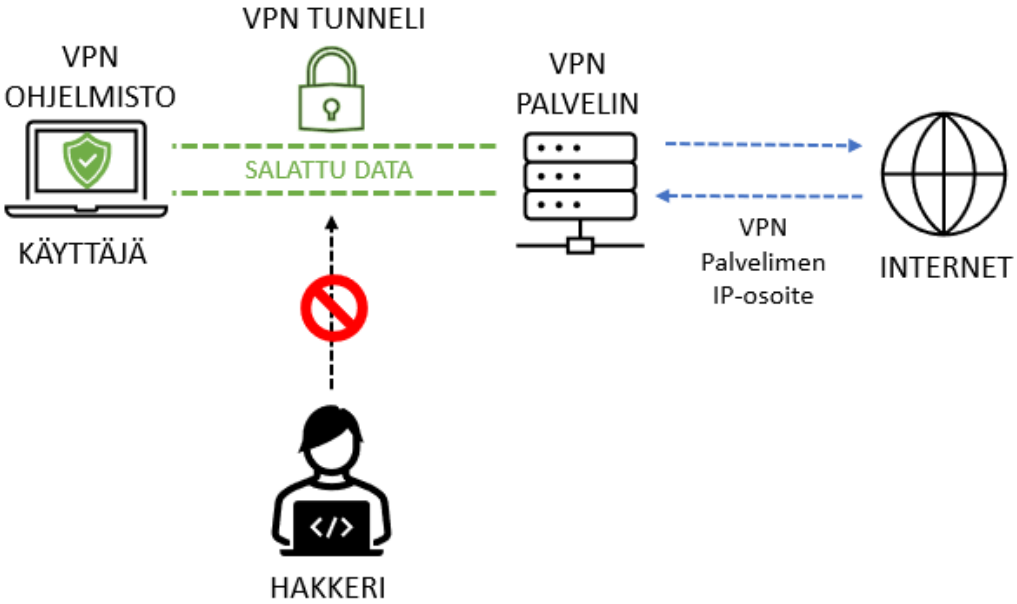
kun taas ulkoisella verkolla viitataan epäluotettavaa verkkoon kuten Internettiin. Palomuuria on mahdollista käyttää kahden tai useamman verkon välillä. Palomuurista on tarjolla erilaisia tyyppejä, jotka eroavat toisistaan verkkoliikenteen suodatus metodien ja toiminnan suorittamiseen käytetyn verkkokerroksen perustella. Palomuurin pääasiallisena tehtävänä on tutkia kaikkea sen läpi kulkevaa verkkoliikennettä sille asetettujen säännösten mukaisesti ja näin estää haitallista ja ei toivottua liikennettä. Palomuurit voivat määritellä hyväksyttävän ja hylättävän liikenteen perustuen verkkoliikenteen pakettien IP-osoitteisiin ja TCP/UDP-portteihin. TCP/UDP-porttien avulla palomuurin on mahdollista tunnistaa, mihin prosessiin tai palveluun verkon paketilla viitataan. Esimerkiksi TCP:n porttinumero 80 kertoo HTTP:n käytöstä. IP-osoitteista palomuuri tarkistaa verkkopaketin lähde ja kohde osoitteen. (Brooks ym. 2018, 207.)

Palomuuri on yleisesti erittäin laajalti käytössä oleva teknologia ja monissa laitteissa se kuuluu osaksi käyttöjärjestelmän sisäänrakennettuja ominaisuuksia. Palomuurin voi kuitenkin myös asentaa laitteelleen osana virustorjuntaohjelmaa tai erillisenä ohjelmistona. Palomuurin käyttäminen on erittäin suositeltavaa, koska se vahvistaa merkittävästi käyttäjien kyberturvallisuutta torjumalla ulkoisesta verkosta tulevia kyberhyökkäyksiä. Palomuuria käytettäessä verkon käyttäjän on hyvä tiedostaa, että palomuuri ei ole yksistään tarpeeksi tehokas teknologia kyberhyökkäyksien torjuntaan. Palomuurin suojausta heikentää se, että haitallisen verkkoliikenteen on mahdollista kiertää palomuuri. Lisäksi palomuuri ei tarjoa täydellistä virustorjuntaa ja sillä ei ole mahdollista suojautua kaikkia uusia uhkia vastaan. Uusien uhkien torjunta ei onnistu, koska palomuuri on suunniteltu havaitsemaan ja torjumaan ennalta tunnettuja hyökkäyksiä. (Chauhan & Jangra 2020, 135-136.) Tästä syystä palomuurin kanssa on hyvä ottaa käyttöön virustorjuntaohjelma, jolla voidaan täydentää palomuurin sisältämiä puutteita.

7.4 VPN

VPN eli Virtual Private Network on teknologia, jolla luodaan erillinen suojattu yksityinen verkko vähemmän turvallisen julkisen verkon kuten Internetin yli. VPN:llä luodussa yksityisessä verkossa tiedonsiirto laitteiden välillä tapahtuu salattuna, jonka ansiosta ulkopuoliset eivät pääse tarkastelemaan verkkoliikenteen sisältöä. VPN:n toteutetaan luomalla verkkoliikenteen kohteen ja lähteen välille oma suojattu tunneli hyödyntämällä tiettyjä tunneloinnin mahdollistavia protokollia. Tunnelissa verkkoliikenne kuljetetaan suojatulle VPN-palvelimelle, jonka kautta se siirtyy lopulliseen kohteeseen verkossa. VPN-palvelimelta eteenpäin lähtiessä liikenteen alkuperäinen IP-osoite vaihdetaan toiseen, minkä ansiosta käyttäjä pysyy anonyymina verkossa. VPN:n tunnelissa liikkuva data suojataan lisäämällä siihen

salaus käyttämällä kryptaukseen soveltuvaa metodia. (Brooks ym. 2018, 550-551.) (KUVA 5.) VPN yhteyden avulla voidaan toteuttaa erityyppisiä VPN-malleja kuten site-to-site VPN ja remote access VPN. Site-to-site VPN-mallia käytetään luodessa yhteys kahden eri verkon välille niiden VPN-yhdyskäytävien avulla. Site-to-site VPN-mallia hyödynnetään usein luotettavien verkkojen välillä kuten esimerkiksi yrityksen eri toimipisteissä olevien verkkojen yhteydessä. Remote access VPN-mallissa VPN-yhteys luodaan yksittäisen käyttäjän ja verkon välille. Remote access VPN-mallia käytetään yleensä silloin, kun käyttäjä yhdistyy turvattomasta verkosta resursseihin, jotka ovat suojatussa verkossa. (Chauhan & Jangra 2020, 279-281.)



KUVA 5. VPN:n toimintaperiaate (mukaillen Pixabay 2019)

VNP:n pääasiallisena tarkoituksena on suojata verkkoyhteyttä ja verkon käyttäjän yksityisyyttä tarjoamalla erilaisia tapoja kyberturvallisuuden vahvistamiseen. VPN-yhteyttä hyödynnetään usein liityttäessä julkisesti tarjolla olevaan Wi-Fi-verkkoon, sillä VPN pystyy salaamaan ja suojaamaan käytettyä yhteyttä. VPN:n avulla pystytään myös piilottamaan IP-osoitteita, vaihtamaan virtuaalista sijaintia ja luomaan helposti etäyhteyksiä toisiin suojattuihin järjestelmiin kuten vaikka työpaikalle. VPN:n käyttöön ottaminen tapahtuu yleensä VPN-palveluja tarjoavan ohjelmiston kautta, joka huolehtii yhteyden muodostamisesta ja viestinnästä VPN-palvelimen kanssa. VPN:n ohjelmistoista löytyy ilmaisia ja maksullisia versioita, joista on suositeltavaa käyttää maksullisia versioita, joka on toteutettu luotettavan palveluntarjoajan toimesta.

7.5 Yleiset salasanojen turvallisuus käytännöt

Salasana on tärkeä osa toimivaa ja turvallista pääsynhallintaa verkossa, sillä se toimii avainasemassa niin käyttäjien yksilöinnissä kuin tunnistuksessa. Salasana toimii yleensä ensisijaisena puolustusmekanismina, kun suojataan verkon käyttäjän yksityisiä ja arvokkaita tietoja eri tileillä verkossa. Salasanojen varaan luotetaan yhä enemmän tärkeitä henkilö- ja tilitietoja, minkä takia niiden turvaaminen on välttämätöntä. Turvalliset salasana käytännöt auttavat suojaamaan itse salasanoja ja tehostamaan salasanoihin kohdistuvien kyberhyökkäysten torjuntaa. Yleinen hyvä käytäntö salasanojen kanssa on, että salasanasta tehdään tarpeeksi pitkä ja monimutkainen. Vahvassa salasanassa tulee olla enemmän kuin kahdeksan merkkiä ja käytetyt merkit sisältävät numeroita, erikoismerkkejä, isoja kirjaimia ja pieniä kirjaimia. Vahvassa salasanassa kannattaa hyödyntää salasanalausetta, joka yhdistää useita sanoja ja merkkisarjoja yhdeksi lauseeksi. Näin salasanaan saadaan enemmän pituutta ja se on helpompi muistaa kuin satunnainen merkkien sarja. Salasanan valinnassa tulee välttää käyttämästä lyhyitä merkkiyhdistelmiä, yksittäisiä sanakirjan sanoja tai pelkkiä numerosarjoja. Erilaisiin henkilökohtaisiin tietoihin kuten nimeen, asuinpaikkaan ja tärkeisiin päivämääriin pohjautuvia salasanoja kannattaa myös välttää.

Luomalla vahvan salasanan verkon käyttäjä parantaa merkittävästi valmiuttaan torjua tilien ja laitteiden salasanoihin kohdistuvia kyberhyökkäyksiä. Vahvan salasanan lisäksi on kuitenkin hyvä huomioida muita toimenpiteitä, jotka vahvistavat salasanan antamaa suojaa. Yleinen ohje turvalliseen salasanan käyttöön on se, että samaa salasanaa ei käytetä useissa eri verkkopalveluissa. Salasanan uudelleenkäyttäminen altistaa helpommin verkon käyttäjän datan suurelle vahingolle, kun yhden tilin murtaminen vaarantaa automaattisesti kaikki muut käytetyt tilit. Salasanan käyttämisessä on tarpeellista muistaa vaihtaa salasanaa ajoittain, sillä ajan kuluessa salasanojen turvallisuus laskee. Salasana tulee vaihtaa myös tilanteissa, jossa tilillä on tapahtunut epäilyttävää toimintaa tai tili on tiedettävästi joutunut osaksi tietomurtoa. Salasanojen kanssa on suositeltavaa ottaa käyttöön aina monivaiheinen tunnistautuminen, jos siihen on mahdollisuus. Monivaiheinen tunnistautuminen eli MFA vaatii käyttäjältä varmistuksen useammasta lähteestä, jotta oikeutettu pääsy verkonpalveluun voidaan virallisesti todistaa. Yksinkertaisesti monivaiheinen tunnistautuminen voidaan toteuttaa lähettämällä kirjautumisen yhteydessä erillinen ilmoitus toiselle laitteelle, josta se pitää hyväksyä ennen kuin kirjautuminen onnistuu.

8 YHTEENVETO

Kyberhyökkäykset ovat aina ajankohtainen aihe, kun tarkastellaan verkkoa ja sen käyttäjiä. Uusia laitteita ja palveluita liittyy verkkoon jatkuvasti ja verkon hyökkäyspinta-ala laajenee vauhdilla. Kasvun seurauksena verkkoon syntyy yhä enemmän mahdollisuuksia erilaisille tietoturva-aukoille, jotka voivat tarjota pääsyn verkossa liikkuvaan arvokkaaseen dataan. Nämä haavoittuvuudet kiinnostavat erityisesti kyberhyökkääjiä, joille nykypäivän monipuolinen verkkoympäristö on luonut entistä enemmän tapoja ja työkaluja kyberhyökkäysten toteuttamiseen. Onnistuneet kyberhyökkäykset tuottavat paljon ongelmia virallisille verkon käyttäjille aiheuttamalla monenlaista vahinkoa verkossa ja sen laitteissa. Tästä syystä kyberhyökkäysten ymmärtämisestä on tullut ensisijaisen tärkeää.

Tämän opinnäytetyön kautta haluttiin tutustua tarkemmin erilaisiin verkossa tapahtuviin kyberhyökkäyksiin ja niiden torjuntakeinoihin. Opinnäytetyön tarkoituksena oli käydä kattavasti läpi osa yleisimmistä kyberhyökkäystyypeistä ja kertoa niiden ominaisuuksista, joiden pohjalta niitä olisi mahdollista tunnistaa verkossa. Opinnäytetyön sisällössä hyökkäyksiä päädyttiin käsittelemään tarkemmin kategorioissa haittaohjelmat, palvelunestohyökkäykset ja muut kyberhyökkäykset. Näissä opinnäytetyön osuuksissa käytiin läpi esiteltyjen kyberhyökkäysten toimintaperiaatetta, leviämistä ja niiden aiheuttamia vaikutuksia. Teorian tarkoituksena oli avata paremmin hyökkäyksiin liittyviä käsitteitä ja antaa hyvä kokonaiskuva siitä, mitä kyberhyökkäys konkreettisesti tekee ja mistä sen voi tunnistaa.

Eri kyberhyökkäysmuotojen lisäksi opinnäytetyössä haluttiin perehtyä hyökkäysten torjuntakeinoihin. Opinnäytetyössä torjuntaa käsittelevässä osuudessa tutustuttiin kyberturvallisuutta vahvistaviin käytäntöihin ja toimintatapoihin mutta myös muutamiin yleisiin ohjelmisto ratkaisuihin, jolla suojausta voidaan lisätä. Opinnäytetyössä kyberhyökkäysten torjuntakeinoja tarkastelevan teorian tarkoituksena oli esitellä yleistasolla torjunnan toimintaan ja kertoa, miten se todellisuudessa suojaa verkon käyttäjää. Päätavoitteena opinnäytetyössä oli käydä lyhyesti mutta kattavasti läpi kyberhyökkäysten teoriaa ja luoda informatiivinen kokonaisuus, jonka kautta aihetta on helppo ymmärtää.

LÄHTEET

Bijalwan, A. 2022. *Network forensics: Privacy and security*. Boca Raton: CRC Press.

Brooks, C. J., Grow, C., Craig, P. & Short, D. 2018. *Cybersecurity essentials*. Indianapolis, IN: Sybex.

Calder, A. 2020. *Cyber Security: Essential Principles to Secure Your Organisation.* IT Governance Ltd. Saatavilla: https://doi.org/10.2307/j.ctv10crcbg. Viitattu 7.4.2023.

Chauhan, S. R. & Jangra, S. 2020. *Computer Security and Encryption: An Introduction*. Mercury Learning & Information. Saatavilla: https://www.proquest.com/docview/2530692539/bookReader?accountid=10007 . Viitattu 4.4.2023.

Dake. 2006. Tcp synflood. CC-BY-SA-2.5. Wikimedia Commons. Saatavilla: https://commons.wikimedia.org/wiki/File:Tcp_synflood.png .

Donaldson, S., Williams, C. & Siegel, S. 2018. *Understanding Security Issues*. DEG Press. Saatavilla: https://doi.org/10.1515/9781501506505. Viitattu 6.4.2023.

Fruhlinger, J. 2022. *What is XSS? Cross-site scripting attacks explained*. CSO (Online). Saatavissa: https://www.proquest.com/docview/2637204256/D5CB9F8DC8AD45D5PQ/1?accountid=10007 . Viitattu 12.4.2023.

Gupta, C. P. & Goyal, K. K. 2020. *Cybersecurity: A Self-Teaching Introduction*. Mercury Learning & Information. Saatavilla: https://www.proquest.com/docview/2440305879/bookReader?accountid=10007&ppg=17 . Viitattu 21.3.2023.

Imperva Incapsula. 2014. Ataque Smurf DDoS. CC-BY-SA-4.0. Wikimedia Commons. Saatavilla: https://commons.wikimedia.org/wiki/File:Ataque_Smurf_DDoS.png .

Jia, W. 2022. Analysis on Password Attack Model and Password Generation. *2022 International Conference on Computers, Information Processing and Advanced Education (CIPAE).* 145-149. Saatavilla: doi: https://doi.org/10.1109/CIPAE55637.2022.00038 . Viitattu: 19.4.2023.

Johnson, D. 2020. What is a computer worm? Here's how to protect yourself from the replicating malware. *Business Insider*. US edition edn, New York. Saatavilla: https://www.proquest.com/docview/2460065048/3CD4315C4C9C4FCAPQ/2?accountid=10007 . Viitattu 17.4.2023.

McDonough, B. 2019. *Cyber Smart: Five Habits to Protect Your Family, Money and Identity from Cyber Criminals*. John Wiley & Sons, Incorporated. Saatavilla: https://www.proquest.com/docview/2159924099/bookReader?accountid=10007&ppg=37 . Viitattu 16.3.2023.

Monnappa K, A. 2018. *Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware*. Packt Publishing, Limited. Saatavilla: https://www.proquest.com/docview/2135170744/bookReader?accountid=10007&ppg=21 . Viitattu 16.3.2023.

Nasanbuyn. 2016. MITM Diagramm. CC-BY-SA-4.0. Wikimedia Commons. Saatavilla: https://commons.wikimedia.org/wiki/File:MITM_Diagramm.png .

Ozkaya, E. 2019. *Cybersecurity: the Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity*. Packt Publishing, Limited. Saatavilla: https://www.proquest.com/docview/2233154713/bookReader?accountid=10007&ppg=99 . Viitattu 14.3.2023.

Pixabay. 2019. Saatavilla: https://pixabay.com/fi/illustrations/vpn-henkil%C3%B6tietoja-suoratoisto-4341596/ .

Sarmah, U., Bhattacharyya, D. K. & Kalita, J. K. 2018. A survey of detection methods for XSS attacks. *Journal of Network and Computer Applications* 118, 113-143. Saatavilla: https://doi.org/10.1016/j.jnca.2018.06.044 . Viitattu 13.4.2023.

Singh, A. 2020. *CyberStrong: A Primer on Cyber Risk Management for Business Managers*. SAGE Publications India Pvt, Ltd. Saatavilla: https://doi.org/10.4135/9789354792625 . Viitattu 9.3.2023.

Sutton, D. 2018. *Business Continuity in a Cyber World: Surviving Cyberattacks*. Business Expert Press. Saatavilla: https://www.proquest.com/docview/2134166625/bookReader?accountid=10007&ppg=8 . Viitattu 31.3.2023.

Swinhoe, D. 2019. What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. *CSO (Online)*. Saatavissa: https://www.proquest.com/docview/2179169535/539D0D4B90E24B3EPQ/2?accountid=10007 . Viitattu 11.4.2023.

Translated by Content Engine, L.L.C. 2022, *How do you know if your computer is infected by a virus or malware?*, English ed. edn, Miami. Saatavilla: https://www.proquest.com/docview/2709508993/41FF29B265594E4BPQ/17?accountid=10007# . Viitattu 21.4.2023.

Waschke, M. 2017. *Personal cybersecurity: How to avoid and recover from cybercrime*. Kustannuspaikka tuntematon: Apress.

Yangchun, Z., Zhao, Y. & Yang, J. 2020. New Virus Infection Technology and Its Detection. *2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)*, 388-394. Saatavissa: https://doi.org/10.1109/ICSESS49938.2020.9237708 . Viitattu 17.4.2023.